

CISO White Paper Series

---

# Privacy and Information Security Regulatory Compliance Guidelines for the Financial Services Industry

***U.S. Treasury Mandates for Data Log Collection,  
Retention, and Investigation***

**Plus Gramm-Leach-Bliley, Sarbanes-Oxley,  
FTC Information Safeguards Rule, California SB 1386**

Updated October, 2003

---

Addamark Technologies, Inc.  
1-415-281-1900  
[compliance@addamark.com](mailto:compliance@addamark.com)  
[www.addamark.com/compliance](http://www.addamark.com/compliance)

# Table of Contents

- Executive Summary ..... 3
- Legislative Action on Information Security and Privacy** ..... 4
  - Gramm-Leach-Bliley (Financial Services Modernization Act of 1999) ..... 4
  - FTC Information Safeguards Regulation..... 5
  - Sarbanes-Oxley Act of 2002..... 5
  - California SB 1386 on Personal Information Privacy ..... 6
  - Other National and International Information Security Regulations ..... 7
- Activities Required for Compliance and Risk Management**..... 7
  - Detecting Insider Abuse and Conducting Thorough Investigations ..... 8
  - Deterring Attacks by Supporting Effective Prosecutions ..... 9
  - Reducing Risks and Liability ..... 10
- Infrastructure Requirements to Achieve Regulatory Compliance**..... 11
- Technology Solutions for Regulatory Compliance**..... 12
- Appendix A - Data Logging Guidelines for the Financial Services Industry ..... 13
- Appendix B - Additional Regulatory Compliance Resources ..... 19

## Executive Summary

Federal and state lawmakers have enacted new regulations for financial organizations designed to protect consumers' private information and establish standards for information security. These include the Gramm-Leach-Bliley Act, the FTC Information Safeguards Regulation, Sarbanes-Oxley, California Senate Bill 1386 on Personal Information Privacy and other national and international information security regulations.

In order to successfully achieve the objectives of the new regulations, organizations must closely monitor user behavior, implement systems to detect data theft, sabotage and insider abuse – and must be able to investigate all logged activities to determine exactly how user data has been used and by whom. These proactive capabilities must be an integral part of a company's standard business processes.

Only when a broad variety of log data from many different network sources is aggregated, stored and analyzed can management be assured that regulations are being followed and internal requirements are being met. Since manual processing and analysis of log data is so difficult, compliance with legislative and regulatory mandates is less expensive and more easily managed when automated long-term audit log archiving and analysis processes are implemented.

Every security event is a serious incident in the financial services industry, and the most significant incidents may be both undetectable and indistinguishable from billions of routine events. Unless detailed logs are readily available to analysts and investigators, regulatory compliance can not be assured. The intent of many regulations is for data logs to be stored in a central location that can be easily, quickly and flexibly queried and archived for the appropriate amount of time (commonly three to six years) as required by regulatory bodies relevant to your industry or business sector.

Since logged events from a wide variety of devices must be stored and remain queryable for a long period of time, existing technology solutions are often inadequate to achieve compliance with the regulations. Existing RDBMS-based data management systems cannot handle the volume of traffic that commonly exists, and various enterprise security management products that rely on RDBMS technology are not an adequate solution.

According to several industry analysts,<sup>1, 2</sup> many financial services firms have failed to implement adequate technology tools needed to achieve full regulatory compliance, either because of the expense or complexity involved.

This paper summarizes the various regulatory measures that have emerged in the wake of elevated privacy concerns, information theft incidents and financial reporting irregularities in recent years, and provides a checklist of federal guidelines on data logging that should be followed by financial organizations to ensure regulatory compliance.

---

<sup>1</sup> Burton Group, "Security Event Management and Auditing Identity Infrastructure," September 9, 2003

<sup>2</sup> Yankee Group, "Identity Management Is the Key to the Enterprise," September 4, 2003

## Legislative Action on Information Security and Privacy

The job of the chief information security officer has become exponentially more complex with the recent passage of strict new federal, state and international regulations governing the security and privacy of financial information. These include the Gramm-Leach-Bliley Act, the FTC Information Safeguards Regulation, the Sarbanes-Oxley Act and California Senate Bill 1386 on Personal Information Privacy. Corporate boards and senior executives have been directed to make sure that security and privacy policies are implemented and maintained. Accountability and potential penalties are placed unambiguously on board members<sup>3</sup> and their designated subordinates, most often IT executives and security professionals.

### Gramm-Leach-Bliley (Financial Services Modernization Act of 1999)

GLBA has spawned a comprehensive set of rules and regulatory measures that address both information privacy and information security, and hold corporate management accountable to evaluate risks and implement adequate technological safeguards to keep information systems secure. Financial services firms and institutions are required to create and implement written information security programs<sup>4</sup> that define how the organization is physically and technologically safeguarding customer information.

Watchdog entities like the Federal Trade Commission, Federal Deposit Insurance Commission, Securities and Exchange Commission, National Association of Securities Dealers, Office of the Comptroller of Currency, Federal Reserve Board, Office of Thrift Supervision, Treasury Department, National Credit Union Administration, Federal Financial Institutions Examination Council and various federal banking agencies are empowered by GLBA to implement and enforce rules and regulations for financial institutions that fall under their jurisdiction.

A number of these agencies have issued similar language. "Any financial institution that provides financial products or services to consumers must comply with the privacy provisions of Subtitle A of Title V of Gramm-Leach-Bliley (codified at 15 U.S.C. §§ 6801-09) and the privacy rules. All companies that provide financial products or services to individuals, not businesses, to be used primarily for personal, family, or household purposes are covered."

This description can be broadly interpreted to include any regulated financial company or business that engages in financial activities including banks, bank holding companies, securities firms, insurance companies, insurance agencies, thrifts, credit unions, mortgage lenders and brokers, finance companies, escrow companies, appraisers, credit reporting companies, title abstractors, insurance companies, notaries and check cashers. Because of the way GLBA defines "financial activities," it may also extend to travel agencies and real estate brokerages.<sup>5</sup>

Financial organizations are required by GLBA to notify their customers of their policies related to disclosing non-public customer information to third parties and affiliates. This notification must be prominent and must be made to all clients when they begin their relationship with the institution and to existing customers on an annual basis. Customers must also be given an opportunity to decline or opt out of having their private information disclosed. Protected information includes names, addresses, phone numbers, credit card numbers, social security data, loan application information and more.

---

<sup>3</sup> U.S. Securities and Exchange Commission, "SEC Initiatives Under Sarbanes-Oxley and Gramm-Leach-Bliley," a speech by SEC Commissioner Cynthia A. Glassman before the ABA Trust, Wealth Management and Marketing Conference, Tampa, FL on February 26, 2003

<sup>4</sup> Federal Financial Institutions Examination Council, "Interagency Guidelines Establishing Standards For Safeguarding Customer Information."

<sup>5</sup> Privacilla.org, "Select Laws and Regulations: The Gramm-Leach-Bliley Act."

Other GLBA language for safeguarding customer information requires institutions to establish “standards relating to administrative, technical and physical information safeguards for financial institutions, to ensure the security and confidentiality of customer records and information, to protect against any anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to such records.”

Financial institutions found in non-compliance with GLBA can be subject to civil penalties of \$100,000 for each violation. The officers and directors of such financial institutions can be held personally liable for civil penalties of \$10,000 for each violation, additional fines in accordance with Title 18 of the U.S. Code, and imprisonment up to five years.

## **FTC Information Safeguards Regulation**

GLBA requires financial institutions located within the U.S. and subject to the FTC jurisdiction to undertake measures to protect the personal information of their U.S. customers and investors. The FTC has jurisdiction over financial institutions that are not otherwise regulated by another federal regulatory body, such as hedge funds, mortgage brokers, loan officers, real estate appraisers, check-cashing businesses, non-bank lenders and other businesses.

The FTC Information Safeguards regulation is separate from GLBA and has a different implementation schedule. Companies are required to “maintain physical, electronic and procedural safeguards that comply with federal regulations to guard nonpublic information.” This regulation also requires that organizations implement and maintain a “comprehensive written information security program” with administrative, technical and physical safeguards to protect customer information.<sup>6</sup>

This rule establishes standards for administrative, technical and physical information safeguards. It requires FTC-regulated financial institutions to adopt a written information security program. Most of these implementations were required to be completed by May 23, 2003.

The FTC advises companies to employ a risk identification and assessment process to identify reasonably foreseeable internal and external risks that threaten the security, confidentiality and integrity of customer information. All aspects of an operation (physical, administrative and technical) should be examined to identify risks that could result in unauthorized disclosure, misuse, loss, theft or destruction of customer information.

## **Sarbanes-Oxley Act of 2002**

Sarbox imposes new duties, accountability standards and penalties for non-compliance on public companies and their executives, directors, auditors, attorneys and securities analysts. The Act requires certification by CEOs and CFOs to accompany periodic reports and financial statements. It also requires disclosure on a “rapid and current basis” of information regarding material changes in the financial condition or operations of a public company as the SEC determines is necessary or useful to investors and in the public interest. This represents a fundamental change in the disclosure obligations for public companies.

---

<sup>6</sup> Federal Trade Commission, Final Privacy Rule, 16CFR § 313.6(a)(8)

A significant section of interest to IT managers and CISOs is Sarbox Section 404, which covers internal controls. It states, in part, “a company’s management (is required) to present an internal control report in the company’s annual report containing: (1) a statement of the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) an assessment, as of the end of the company’s most recent fiscal year, of the effectiveness of the company’s internal control structure and procedures for financial reporting. This section also requires the company’s registered public accounting firm to attest to, and report on, management’s assessment.

The original deadline for section 404 compliance was fall, 2003, but the SEC extended the deadline to June 15, 2004 for most large U.S. companies and to April 15, 2005 for small businesses and some foreign organizations. At one extreme, Sarbox provides for penalties of up to \$5 million in fines and 20 years in prison for significant violations, mostly related to accounting fraud. Smaller penalties can be applied for non-compliance when information systems are not kept secure.

### **California SB 1386 on Personal Information Privacy**

The GLB Act of 1999 and other privacy regulations do not require enterprises to notify their customers when personal or private information is compromised, and there is no overriding federal law protecting individual privacy. Such privacy laws have generally been left up to state legislatures. California SB 1386 requires all organizations that possess unencrypted personal data of California citizens to make a full disclosure if the security of that data is compromised at any time. The law is directed at all companies that do business with people living in California, even if the company is located outside California.

Since most large organizations do business in California in one way or another, industry analysts advise that any organization with data on California residents that has a security breach should immediately notify customers of that breach, or risk violating the California law. Companies should also be prepared with strong incident response and easily accessed audit trails in order to comply with California SB 1386.

As an example, an August 2003 report by Giga Research <sup>7</sup> says that companies affected by security incidents such as the MSBlast/LoveSan or “Blaster” worm should investigate all audit trails protected by SB 1386 to meet disclosure requirements. Giga recommended that companies deploy log aggregation, retention and investigation technologies from companies such as Addamark Technologies to comply with California law.

Giga Research analyst Michael Rasmussen says that many companies have a false sense of security that firewalls will protect them from these attacks. But the Blaster worm demonstrated that firewall security measures are not enough to prevent worms from infecting systems. Organizations that do not collect detailed log and event information as part of their audit trail are left exposed to legal ramifications such as non-compliance actions and class action lawsuits, according to Giga.

Federal legislation very similar to California SB 1386 was introduced in the U.S. Senate in June, 2003. If passed, the Notification of Risk to Personal Data Act (NORPDA) would require all U.S. businesses and government agencies to notify customers in the event of a network security breach. Penalties are \$5,000 per violation, up to \$25,000 per day. <sup>8</sup>

---

<sup>7</sup> Giga Research, “Microsoft Blast/LoveSan Worm,” August 15, 2003

<sup>8</sup> United States Senate Press Release, “Senator Feinstein Seeks to Ensure Individuals are Notified when Personal Information is Stolen from Databases,” June 26, 2003

## Other National and International Information Security Regulations

Financial organizations should also be familiar with additional rules that may affect their operations. These may include:

**ISO 17799 Information Security Standard** - An industry standard for information security designed to provide organizations with best practices for information security. It includes such topics as organizational security, asset control, personal security, communications, user access controls and cryptography. Full compliance with this standard requires a number of layers of security procedures and integrated technologies to ensure a highly secure environment for information, assets, employees and partners.

**Basel II Accords** - Directed at international financial institutions by the Basel Committee on Banking Supervision. IT executives should be aware of the Basel II Accords' focus on operational risk. The Banking Supervision Committee has agreed upon a common definition of operational risk as "the risk of direct or indirect loss resulting from inadequate or failed internal process, people and systems, or from external events." This is a clear reference to IT security. Compliance is mandatory starting in 2005, and the requirements outline a need for strong network authentication, authorization and a clear audit trail of all access to confidential customer information and banking records.

**FDA U.S. 21 CFR Part 11** - This regulation from the Food and Drug Administration affects primarily pharmaceutical companies and health care companies, but could also impact accounting firms and financial services companies who serve these industries. It is intended to create criteria for electronic record-keeping technologies while preserving the FDA's ability to protect and promote the public health by facilitating timely review and approval of safe and effective new medical products, conducting efficient audits of records, and pursuing regulatory actions.

**Federal Information Security Management Act of 2002 (FISMA)** - Directed at governmental organizations, it is designed to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. It recognizes the highly networked nature of the Federal computing environment and is intended to provide effective government-wide management and oversight of related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities.

## Activities Required for Compliance and Risk Management

The overarching goals of recently enacted laws and regulations are to protect consumers' private information and establish common standards for information security across all entities within certain industries or industry segments.

Among the fundamental elements of protecting private information are the physical security measures of placing padlocks on file cabinets and securing data centers inside protected buildings. Most companies addressed these physical security issues long ago. From a technology standpoint, basic security tools include firewalls, passwords and integrated authentication and access controls. And it's essential to continuously monitor all users on the corporate network: who's accessing what files, who's looking at information they ought not to be, who's looking at too many sensitive files or personal records.

New information security laws and privacy regulations cannot be met without easy access to detailed activity log data to support a high rate of incident detection and timely incident response. According to Burton Group,<sup>9</sup> “Without properly archived audit data, enterprises will be unable to conduct analyses, investigations, or other reporting functions at a later date.”

Because of the comprehensiveness of the new rules, compliance cannot be achieved with locks, keys, security management applications and intrusion detection systems alone. Full compliance requires a more complete understanding of everything that is happening on all systems throughout the corporate network, and a fully archived record of all activity.

For example, insider abuse is not likely to be detected by perimeter defenses. An authorized insider may have legitimate access to all the resources needed to misappropriate confidential information or perform sabotage. Only by detecting suspicious patterns can analysts uncover inappropriate insider activities. A simple virus may cause havoc in a network unless a company can investigate all of the systems and devices that may have been penetrated and what private records may have been accessed or modified.

In order to minimize these risks and comply with regulations, companies must have detailed visibility to all activities on their systems and networks. They must conduct quick and thorough investigations of every suspicious incident and continuously run queries to detect unusual patterns across a variety of systems and devices. This requires complete visibility of aggregated long-term event history from a wide range of logs and data sources, coupled with a potent ability to make queries to investigate and find hidden patterns.

## **Detecting Insider Abuse and Conducting Thorough Investigations**

When information theft and sabotage is examined closely, the most prominent threats are from inside the enterprise, not outside. Studies by industry analysts and security experts vary slightly, but show a trend of 60 to 80 percent of all security damage coming from inside sources, usually employees. According to the Gartner Group,<sup>10</sup> “insider attacks are responsible for the bulk of financial losses caused by security breaches. Further, insiders cause 70 percent of cyber attacks costing the victim \$20,000 or more. Information security personnel must be fastidious in managing and monitoring critical enterprise system logs. Collecting, analyzing and making sense of multiple systems’ log files is a time-consuming task requiring skill and patience.”

It is essential for companies to routinely monitor inside users’ authorized activities and look for patterns that indicate that protected information or private records may be compromised. Regular system queries should be run routinely as part of the company’s standard daily business processes. Analysts should examine all queries, or at least those that generate alerts or show unusual patterns, such as one employee accessing a much higher number of confidential accounts relative to his or her peers.

Traditional security software applications record events that indicate when a network is being attacked from the outside. They look for errors or anomalies, or a signal from an application or device that indicates something unusual is occurring. Clear, unambiguous instances of information theft, sabotage and abuse are rare. More commonly, the security software detects a lot of normal traffic, which in a larger context may be seen as wrong. It may discover that a particular user is attempting to log into applications where he has no legitimate business.

---

<sup>9</sup> Burton Group, “Security Event Management and Auditing Identity Infrastructure,” September 9, 2003

<sup>10</sup> Report by John Pescatore, Research Director for Internet Security, Gartner Group

In order to do this, analysts must review a lot of very normal looking traffic, or what may look normal at the time. If the organization suspects that a person has done something inappropriate, there may be need to review otherwise routine data logs far into the past. This can be achieved only if a great deal of data from many different sources, devices and applications has been stored in an easily accessible, long-term central repository.

Thorough information security requires detection and prompt investigation. Without an investigation, successful accesses to sensitive documents by an information thief isn't distinguishable from a simple lark by a random hacker, and an organization can't take appropriate steps to contain the impact of the information loss and prosecute the perpetrator. A central data log repository that aggregates together all data log sources provides a framework for effective investigations into suspected insider data theft, sabotage and abuse. Query and correlation capabilities enable security analysts to see summary views of activities, and drill down on a particular user, application or server.

Security threats from outside the organization require a similar set of forensics resources. There's rarely a loud and clear signal that a hacker has infiltrated a system or attacked a firewall. More commonly, these events are detected by reviewing large volumes of seemingly legitimate activities that can be seen as attacks only when they're viewed in a larger context.

When a security analyst is alerted to a potential breach, she or he needs to examine information from many different devices and systems to try and determine what has happened. As an example, when a network intrusion detection system has identified a suspicious request directed against a Web server, the analyst must review that request in conjunction with the Web server log files.

If a Web application is connected to a back-end database that includes customer order information, the analyst might want to view that database log in conjunction with other data log types. The logical steps that the security analyst will follow are difficult to predict in advance. He'll proactively hunt down forensic data and clues, and when he sees something that doesn't look right, he'll try to make sense of it. To complete a full and adequate analytic process, the analyst will need a consolidated view of all of security data logs within a single investigation engine.

## **Deterring Attacks by Supporting Effective Prosecutions**

Security experts believe that one of the best ways to deter information abuse and network attacks is to support effective, ubiquitous prosecution of every serious offense.<sup>11</sup> When employees and outside attackers know that powerful safeguards are in place on a network that catch a very high percentage of offenders, they're much less likely to attempt something inappropriate or illegal. The deterrent value of swift, public prosecutions should not be underestimated.

In recent years, lawmakers have taken a strong interest in intellectual property crimes as well as intellectual property law in general. The federal government has enacted stiff new penalties for intellectual property crimes and theft of computer network-based data.

Security event logs are computer records by definition, and this may affect their admissibility in court actions. Computer records have sometimes been considered to be hearsay, or unreliable evidence. The business records exception rule (Federal Rules of Evidence § 803 (6)) addresses this issue, and event logs may be exempted from hearsay provisions if they are generated as a routine part of business operations.

---

<sup>11</sup> United States Department of Justice, United States Attorneys' Bulletin, Computer Crimes and Intellectual Property, Volume 49, March, 2001

Organizations should seek professional legal guidance on capturing and storing data logs in an appropriate manner to ensure that they can be used as evidence. Legal opinions vary regarding precisely what must be done and the law is not completely clear in this area. However, the one recommendation that appears most frequently in analyst guidance about evidence rules is that security event logging should be a part of every financial organization's routine business practices. Companies that attempt to gather evidence after the fact – after a breach has occurred – stand the greatest chance of having their evidence disallowed.

Protecting the admissibility of electronic evidence is a key point worth repeating. Procedures must be implemented well in advance of any effort to use logging data as evidence in a prosecution or defense action. If a company waits until a system is compromised or a security event occurs before it starts saving logs, those logs may not be admissible in court. They must be able to show there is a routine process by which evidence or logs are stored, and they must be able to document that process as part of their normal business routine.<sup>12</sup>

An August 2003 memo from Giga Research<sup>13</sup> advised, "Organizations should define their evidence discovery policies and procedures and invest in tools that will help facilitate the process. Policies for electronic evidence discovery should define individual responsibility and how requests are to be handled and resolved – not having this defined can be embarrassing and lead to damages for the mishandling of evidence."

According to Giga, an increase in requests for electronic evidence discovery requests is expected as a result of new legislation such as California SB 1386, Sarbanes-Oxley, the USA Patriot Act and Gramm-Leach-Bliley. Giga recommends the implementation of network and system forensic analysis tools, data log retention and investigation tools, and a broad set of database and transaction management systems, document management systems and backup/data recovery systems.

## **Reducing Risks and Liability**

Information security and privacy regulations enacted recently by state and federal authorities have raised these issues to a higher level of visibility. Some industry analysts believe it's just a matter of time until court cases are filed against companies that have not performed appropriate due diligence and have experienced security breaches as a result.

Conscientious information security executives will want to implement all appropriate security measures to comply with all relevant regulations. Yet, the complexity of the systems they manage and the newness of the rules they must follow create a pressing set of challenges around mitigating damages and supporting the recovery and containment of security breaches.

Both civil liability lawsuits and regulatory compliance prosecutions can result when appropriate and adequate security measures are not in place. The best way for organizations to protect themselves against both of these contingencies is to carefully implement all available best-of-breed precautions that fit within an established data security budget.

---

<sup>12</sup> For more details on rules of evidence, see <http://www.law.cornell.edu/rules/fre/803.html>, especially item 6.

<sup>13</sup> Giga Research, IdeaByte, Michael Rasmussen, "Electronic Evidence Discovery," August 28, 2003

## Infrastructure Requirements to Achieve Regulatory Compliance

Some of the new regulations are very specific with their mandates for retaining activity logs. But they're not always so clear on the requirements for how long logs must be saved. In some industries, such as investment brokerage, regulations require that broker-dealers retain some records as long as six years. These include external and internal electronic mail messages, which must be retained and produced within one day when requested by on-site SEC examiners (see sidebars at right and on page 12).

Industry best practices dictate that organizations retain all activity logs in an online repository for at least three years, or six years if reasonable and appropriate. These should be considered minimum standards to support investigations into the misappropriation or misuse of confidential data records.

Addamark's data logging technology makes it reasonable and cost effective to retain all activity logs in a queryable online repository for many years.<sup>14</sup>

Accessible stored data can include logs from dozens or hundreds of different sources including security software, VPNs, firewalls, e-mail servers, Web servers, proxy servers, custom applications, databases, routers, switches and other network devices and systems.

Some of the most useful security and privacy compliance information for financial institutions has been published by the Federal Financial Institutions Examination Council ([www.ffiec.gov](http://www.ffiec.gov)). The FFIEC is an interagency body empowered to prescribe uniform principles, standards and report forms for the federal examination of financial institutions by multiple agencies and make recommendations to promote uniformity in the supervision of financial institutions.



### What Data Logs Should be Saved?

#### ***According to the Federal Financial Institutions Examination Council (FFIEC),***

"An institution's ongoing security risk assessment process should evaluate the adequacy of the system logging and the type of information collected. Security policies should address the proper handling and analysis of log files. Institutions have to make risk-based decisions on where and when to log activity. The following data are typically logged to some extent including:

- Inbound and outbound Internet traffic
- Internal network traffic
- Firewall events
- Intrusion detection system events
- Network and host performance
- Operating system access (especially high-level administrative or root access)
- Application access (especially users and objects with write-and-execute privileges)
- Remote access

When evaluating whether and what data to log, institutions should consider the importance of the related system or information, the importance of monitoring the access controls, the value of logged data in restoring a compromised system, and the means to effectively analyze the data. Logs should capture source identification information; session ID; terminal ID; and the date, time, and the nature of the access attempt, service request, or process.

Many hardware and software products come with logging disabled and may have inadequate log analysis and reporting capabilities. Institutions may have to enable the logging capabilities and then verify that logging remains enabled after rebooting. In some cases, additional software will provide the only means to analyze the log files effectively."

<sup>14</sup> Addamark Technologies, "Building Systems to Manage Event Log Data, Total Cost of Ownership Comparison," July, 2002.

## Technology Solutions for Regulatory Compliance

Financial services firms are common targets for information theft and sabotage due to the high volume of sensitive information that they handle each day and the potential value of stolen information. In other industries, system availability is an overriding concern and one incident matters less than consistent uptime. CISOs in financial services companies own the challenging responsibility of ensuring that every single access to sensitive data is completely legitimate and justifiable.

Every security event is a serious incident in the financial services industry, and the most significant incidents may be both undetectable and indistinguishable from billions of routine events. Until recently, there has been no solution capable of meeting the twin challenges of routinely analyzing terabytes of log data to find the most threatening security incidents and providing flexible query access to data logs to thoroughly investigate every security alert.

Addamark facilitates legal and audit compliance for log retention and investigation. It provides technology solutions that meet or exceed regulatory requirements by storing all logs from all sources in their full, original detail and providing flexible query capability. Addamark provides efficient storage to make retaining many years of raw logs feasible and cost-effective.

By tracking all data types over time with no degradation in performance, these solutions provide the foundation for a more effective network security solution. Scalable parallel architecture enables central storage of historical and unfiltered details. Any log format can be stored; the system is pre-configured for many security and network devices and applications. Other log sources and formats are rapidly supported. The data is stored in a format optimized for event logs, enabling efficient storage of huge amounts of data while providing high availability through redundancy.



### How Long Should Data Logs Be Saved?

*Speaking before an SEC Rules Compliance Conference for Securities Broker-Dealers on March 24, 2003, SEC Associate Director Mary Ann Gadziala provided this interpretation:*

“First, what does prompt records production mean? It means that information requested by examiners on-site should generally be produced on the day requested; however, if information requested is unusually voluminous or complex, firms should discuss with the examiner a mutually agreeable time-frame for production of the documents.

Second, all records of the firm are covered. Not just those specifically required by rule to be made and kept, but all records; this would include exception reports and any other firm records regardless of whether they are required by rule to be created.

Third, electronic messages, including internal and external business-related e-mails must be kept and produced when requested by examiners.

Fourth, while firms may keep records electronically rather than in hard copy, the records must be non-erasable, non-rewriteable, organized, and immediately produced or reproduced. (Rule 17a-4(f))

Fifth, the records must be kept for the requisite period of time, typically three or six years, as specified by rule depending on the type of information. It is not sufficient, for example, to keep records of e-mails for a number of months or a year and then re-use or write over the tapes.”

## Appendix A - Data Logging Guidelines for the Financial Services Industry

Source: Federal Financial Institutions Examination Council

The Federal Financial Institutions Examination Council is an interagency body created to prescribe uniform principles, standards and reports for the examination of financial institutions by various federal agencies. The council has been chartered by the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS) to make recommendations to promote uniformity in the federal supervision of financial institutions.

The FFIEC has published a detailed document that provides explicit guidelines on information security for financial institutions that fall under the jurisdiction of the federal government. The complete document is 118 pages in length and contains over 40,000 words. It can be found on the FFIEC Web site at [www.ffiec.gov](http://www.ffiec.gov), or requested from Addamark Technologies. Please send your request via email to: [compliance@addamark.com](mailto:compliance@addamark.com).

As a convenience to readers of this white paper, the following pages contain excerpts from the FFIEC document related to data logging and network access monitoring. These references have been edited for brevity. Readers are encouraged to refer to the original pages in the FFIEC document to view these guidelines within their full context.

---

### Information Security - IT Examination Handbook - December 2002 Published by the Federal Financial Institutions Examination Council

FFIEC Guideline Description and Reference Page	Addressed by OmniSight
<p><i>Page 16...</i> Authorization for privileged access should be tightly controlled. Privileged access refers to the ability to override system or application controls. Good practices for controlling privileged access include</p> <ul style="list-style-type: none"><li>- Logging and auditing the use of privileged access,</li></ul>	<p>✓</p> <p>✓</p>
<p><i>Pages 23-24...</i> When utilizing PKI policies and controls, financial institutions need to consider the following:</p> <ul style="list-style-type: none"><li>- Recording in a secure audit log all significant events performed by the CA (certificate authority) system, including the use of the root key, where each entry is time/date stamped and signed;</li><li>- Regularly reviewing exception reports and system activity by the CA's employees to detect malfunctions and unauthorized activities; and</li></ul>	<p>✓</p> <p>✓</p>
<p><i>Page 32...</i> DNS hosts, routers and switches are computers with their own operating system. If successfully attacked, they can allow traffic to be monitored or redirected. Financial institutions must restrict, log, and monitor administrative access to these devices.</p>	<p>✓</p>

**Federal Financial Institutions Examination Council: Data Logging Guidelines, Cont'd**

FFIEC Guideline Description and Reference Page	Addressed by OmniSight
<p><i>Page 38...</i>            Given the importance of firewalls as a means of access control, good practices include...            - Logging activity, with daily administrator review (see “Logging and Data Collection”);</p>	<p style="text-align: center;">✓</p>
<p><i>Pages 39-40...</i>            Financial institutions should secure access to the operating systems of all system components by            -- Logging and monitoring user or program access to sensitive resources and alerting on security events,            The critical aspects for access control software, whether included in the operating system or additional security software, are that management has the capability to            - Log user or program access to sensitive system resources including files, programs, processes, or operating system parameters; and            - Filter logs for potential security events and provide adequate reporting and alerting capabilities.</p> <p>Additional operating system access controls include the following actions.            - Activate and utilize operating system security and logging capabilities and supplement with additional security software where supported by the risk assessment process.            - Restrict and log access to system utilities, especially those with data altering capabilities.            - Monitor operating system access by user, terminal, date, and time of access.</p>	<p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p>
<p><i>Page 41-42...</i>            Financial institutions should control access to applications by...            - Logging access and security events, and            - Using software that enables rapid analysis of user activities.            - Logging access and events (see “Logging and Data Collection”).</p>	<p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p>
<p><i>Pages 43-44...</i>            Financial institutions should secure remote access to and from their systems by            - Logging and monitoring remote access,            Good controls for remote access include the following actions.            - Log and monitor the date, time, user, user location, duration, and purpose for all remote access.</p>	<p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p>
<p><i>Page 55...</i>            Financial institutions should ensure that systems are developed, acquired, and maintained with appropriate security controls. The steps include...            - Incorporating appropriate security controls, audit trails, and logs for data entry and data processing; Implementing an effective change control process;</p>	<p style="text-align: center;">✓</p>



## Federal Financial Institutions Examination Council: Data Logging Guidelines, Cont'd

FFIEC Guideline Description and Reference Page	Addressed by OmniSight
<p><i>Pages 64-66, con'd</i> Some considerations for securing the integrity of log files include</p> <ul style="list-style-type: none"> <li>- Encrypting log files that contain sensitive data or that are transmitting over the network,</li> <li>- Ensuring adequate storage capacity to avoid gaps in data gathering,</li> <li>- Securing backup and disposal of log files</li> <li>- Logging the data to a separate, isolated computer,</li> <li>- Logging the data to write-only media like a write-once/read-many (WORM) disk or drive,</li> <li>- Utilizing centralized logging, such as the UNIX "SYSLOG" utility, and</li> <li>- Setting logging parameters to disallow any modification to previously written data.</li> </ul> <p>The financial institution should have an effective means of tracing a security event through their system. Synchronized time stamps on network devices may be necessary to gather consistent logs and a consistent audit trail. Additionally, logs should be available, when needed, for incident detection, analysis and response.</p>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> <li>✓</li> </ul>
<p><i>Page 68...</i> Intrusion Detection and Response Financial institutions should have the capability to detect and respond to an information system intrusion commensurate with risk...</p> <p>--Response to an intrusion, including the containment and restoration of systems and appropriate reporting.</p>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> </ul>
<p><i>Page 72...</i> ...remote access logs can be reviewed daily for access during unusual times. Other logs can be reviewed on other regular cycles for other unusual behaviors...</p> <p>Central reporting and analysis of all IDS output, honeypot monitoring, and anomalous system behavior assists in the intrusion identification process.</p>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> </ul>
<p><i>Pages 82-83...</i> Monitoring and Updating...</p> <ul style="list-style-type: none"> <li>- Security personnel should monitor the information technology environment and review performance reports to identify trends, new threats, or control deficiencies. Specific activities could include reviewing security and activity logs, investigating operational anomalies, and routinely reviewing system and application access levels...</li> <li>- Security personnel should have access to automated tools appropriate for the complexity of the financial institution systems. Automated security policy and security log analysis tools can significantly increase the effectiveness and productivity of security personnel.</li> </ul>	<ul style="list-style-type: none"> <li>✓</li> <li>✓</li> </ul>

**Federal Financial Institutions Examination Council: Data Logging Guidelines, Cont'd**

FFIEC Guideline Description and Reference Page	Addressed by OmniSight
<p><i>Pages A-3 and A-4</i>            Determine the adequacy of the risk assessment process.</p> <ul style="list-style-type: none"> <li>• Network Access - Network access controls including firewalls - Appropriate application access controls - Remote access controls including wireless, VPN, modems, and Internet-based</li> <li>• Host Systems - Secure configuration (hardening) - Operating system access - Application access and configuration - Malicious code prevention - Logging - Monitoring and updating</li> <li>• User Equipment - Secure configuration (hardening) - Operating system access - Application access and configuration - Malicious code prevention - Logging - Monitoring and updating</li> <li>• Physical controls over access to hardware, software, storage media, paper records, and facilities.</li> <li>• Intrusion detection and response</li> </ul>	<p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p>
<p><i>Pages A -12 and A-13...</i></p> <ul style="list-style-type: none"> <li>- Evaluate the appropriateness of technical controls mediating access between security domains. Consider               <ul style="list-style-type: none"> <li>• Firewall topology and architecture</li> <li>• Type(s) of firewall(s) being utilized</li> <li>• Physical placement of firewall components</li> <li>• Monitoring of firewall traffic</li> </ul> </li> <li>- Determine whether logs of security-related events are sufficient to affix accountability for network activities, as well as support intrusion forensics and IDS. Additionally, determine that adequate clock synchronization takes place.</li> <li>- Determine if logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.</li> </ul>	<p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p>
<p><i>Page A -14...</i>            Determine whether remote access devices and network access points for remote equipment are appropriately controlled.</p> <p>-- Appropriate logging and monitoring takes place.</p>	<p style="text-align: center;">✓</p>
<p><i>Page A -15...</i></p> <ul style="list-style-type: none"> <li>- Determine whether logs are sufficient to affix accountability for host activities and to support intrusion forensics and IDS and are appropriately secured for a sufficient time period.</li> </ul>	<p style="text-align: center;">✓</p>
<p><i>Page... A -18...</i></p> <ul style="list-style-type: none"> <li>-Review security procedures for daily and periodic report monitoring to identify unauthorized or unusual activities.</li> </ul>	<p style="text-align: center;">✓</p>
<p><i>Page A -19...</i></p> <ul style="list-style-type: none"> <li>- Determine whether logs of security-related events are sufficient to assign accountability for intrusion detection system activities, as well as support intrusion forensics and IDS.</li> <li>- Determine if logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.</li> </ul>	<p style="text-align: center;">✓</p> <p style="text-align: center;">✓</p>

**Note:**

**The preceding five pages within Appendix A contain excerpts from published FFIEC guidelines related to data logging. These references have been edited for brevity. Readers are encouraged to refer to the original pages in the FFIEC document to view these references within their full context.**

**The complete 118 page FFIEC guidelines document for financial institutions is available by request from Addamark Technologies (send your request to: [compliance@addamark.com](mailto:compliance@addamark.com)), or visit the FFIEC Web site at [www.ffiec.gov](http://www.ffiec.gov)**

## Appendix B - Additional Regulatory Compliance Resources

American Bankers Association - <http://www.aba.com/compliance/default.htm>

CERT Coordination Center - <http://www.cert.org>

Code of Federal Regulations (CFR) - <http://www.gpoaccess.gov/cfr/>

Computer Security Resource Center - <http://csrc.nist.gov/publications>

Cornell Legal Information Institute - <http://www.law.cornell.edu>

Electronic Privacy Information Center on GLBA - <http://www.epic.org/privacy/glba>

Federal Computer Incident Response Center - <http://www.fedcirc.gov>

Federal Financial Institutions Examining Center - <http://www.ffiec.gov>

Federal Register - <http://www.gpoaccess.gov/fr/index.html>

FindLaw - <http://www.findlaw.com>

FTC Guidance on GLBA - <http://www.ftc.gov/privacy/glbact>

Information Systems Security Association - [www.issa.org](http://www.issa.org)

ISO 17799 Best Practices in Information Security - <http://www.iso-17799.com>

National Association of Federal Credit Unions - <http://www.nafcu.org>

National Association of Securities Dealers - <http://www.nasd.com/>

National Infrastructure Protection Center - <http://www.nipc.gov>

Office for Regulatory Audits and Compliance - <http://www.ofrac.com>

Privacilla on GLBA - <http://www.privacilla.org/business/financial/glb.html>

SANS Institute - <http://www.sans.org>

SEC Security Rules - <http://www.sec.gov/rules/final.shtml>

SEC Associate Director's Remarks on Records Compliance -  
<http://www.sec.gov/news/speech/spch032403mag.htm>

Thomas, Legislative Information on the Internet - <http://thomas.loc.gov>

U.S. Code (USC) - <http://www.gpoaccess.gov/uscode/index.html>